

## REMARKS

### **I. INTRODUCTION**

No new matter has been added. Thus, claims 1- 4 remain pending in this application. It is respectfully submitted that based on the following remarks, all of the presently pending claims are in condition for allowance.

### **II. THE 35 U.S.C. § 103(a) REJECTIONS SHOULD BE WITHDRAWN**

Claims 1-4 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 7,013,391 to Herle et al. (hereinafter “Herle”). (See 02/22/08 Office Action, p. 3).

Herle includes a mobile station location server that determines a mobile station’s location through various locating techniques or by receiving the location information from the mobile station over an encrypted channel. The server stores the location in memory that may be accessed by authorized client access devices. A requesting client access device transmits a request to the server. The server authenticates the request to verify that the client access device is authorized to receive the location information. If the client access device is authorized, the server can then transmit the information in either an encrypted or decrypted form to the device. (See Herle, Abstract.) The server also holds within its memory profile fields of the mobile stations, authorized client profile fields, and encryption-decryption keys. (See Herle col. 5, ll. 55-57.) Using the different fields and keys, the server authenticates and transmits the location information. (See Herle col. 5, l. 59 – col. 6, l. 8.)

Claim 1 recites, “sharing the predetermined encryption key between the mobile device and the remote terminal **but not with the server.**” The Examiner asserts, “that which would have make obvious to one of ordinary skill in the art at the time the invention was made to see the suggestion of another embodiment implementation of the invention wherein the MS does not share with the server the use of the encryption-decryption key.” (See 02/22/08 Office Action p. 4-5). Applicant respectfully disagrees.

Herle states that, “Wireless mobile stations will soon be required to be able to determine their geographic location. This location information is required to be relayed **only to the wireless service provider or a Public Service Access Point**... While this position is necessary for emergency purposes, it would also be useful for targeting commercial services.” (See Herle col. 1, ll. 17-32). Herle further states that, “The present invention encompasses an apparatus for transferring geographic location information associated with the mobile station to a **server** accessible via a communication network coupled to the wireless network. The apparatus comprises memory that stores mobile station current position information **and at least one encryption/decryption key**.” (See Herle col. 1, ll. 45-50).

The Examiner asserts that “not sharing the encryption key with the server,” as recited in claim 1, is taught by Herle in “MS position server application program may also be responsible for controlling access to mobile station database 360.” (See Office Action 2/22/2008 p. 4). However, Herle, within the same paragraph, states that “[f]or example, if a request is received for location information for a particular mobile station, that request **must contain a proper decryption key**. MS position server application program determines if that decryption key is accurate so that the requesting entity can access the location information.” (See Herle, col. 6, ll. 3-8). This clearly is not equivalent to “sharing the predetermined encryption key between the mobile device and the remote terminal **but not with the server**.” In contrast, Herle states that the server determines if the decryption key is accurate before allowing the requesting entity to access the location information.

Herle contradicts the Examiner’s assertion that at the time of the invention one of ordinary skill would have made an embodiment that prevented the server from having access to the encryption/decryption key. Herle specifically states that the server “contains ... encryption-decryption key(s) 363.” (See Herle col. 5, ll 55-57). In contrast, claim 1 recites, “sharing the predetermined encryption key between the mobile device and the remote terminal **but not with the server**.” Furthermore, Herle states that when a request is made the server will “authenticate the client access ... if the client access device properly authenticates ... server transmits the encrypted MS 111 position data” or “MS location server 160 decrypts the MS 111 position data and transmits unencrypted MS 111 position data to authenticated client device.” (See Herle col.

6, ll. 48-60). In either embodiment, Herle stores the encryption/decryption key so that it is able to decrypt the position. In contrast to claim 1 which recites, “sharing the predetermined encryption key between the mobile device and the remote terminal **but not with the server.**”

Additionally, the Examiner in responding to similar previous arguments stated that “the applicant . . . should understand that the statement previously quoted does not exclude from the invention the embodiment described by Herle in which the mobile station shares its encryption key with the remote mobile station only.” (See Office Action 2/22/2008 p. 2). Applicant respectfully disagrees with the Examiner’s characterization of Herle’s teaching. The cited portion of Herle relied on by the Examiner states that the mobile station gives out its location only to those having authorization from the mobile station user. However, all the embodiments of Herle teach that the interface for all the mobile stations is the server to obtain this information and the server has the encryption key. There is no embodiment described or suggested in Herle where the encryption key is not shared with the server. Therefore, Applicant submits that claim 1 is patentable over Herle.

Independent claim 2 recites, “A mobile device configured to determine its location, encrypt its location using an encryption key, transmit the encrypted location to a server, and share the predetermined encryption key with a remote terminal but not the server.” Applicant submits that this claim is also allowable for at least the same reasons given above with respect to claim 1.

Independent claim 3 recites, “wherein between receipt and transmission of the encrypted location by the server, the server is not in possession of the encryption key.” Applicant submits that this claim is also allowable for at least the same reasons given above with respect to claim 1.

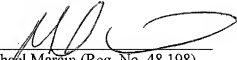
Independent claim 4 recites, “A terminal configured to query a remote server for the location of a particular mobile device with which it has shared an encryption key independently of the server; and upon receipt of an encrypted location encrypted with the encryption key, decrypting the location.” Applicant submits that this claim is also allowable for at least the same reasons given above with respect to claim 1.

**CONCLUSION**

In view of the above remarks, it is respectfully submitted that all the presently pending claims are in condition for allowance. All issues raised by the Examiner having been addressed, an early and favorable action on the merits is earnestly solicited.

Respectfully submitted,

Dated: April 21, 2008

By:   
Michael Marcín (Reg. No. 48,198)

Fay Kaplun & Marcín, LLP  
150 Broadway, Suite 702  
New York, NY 10038  
Phone: 212-619-6000  
Fax: 212-619-0276